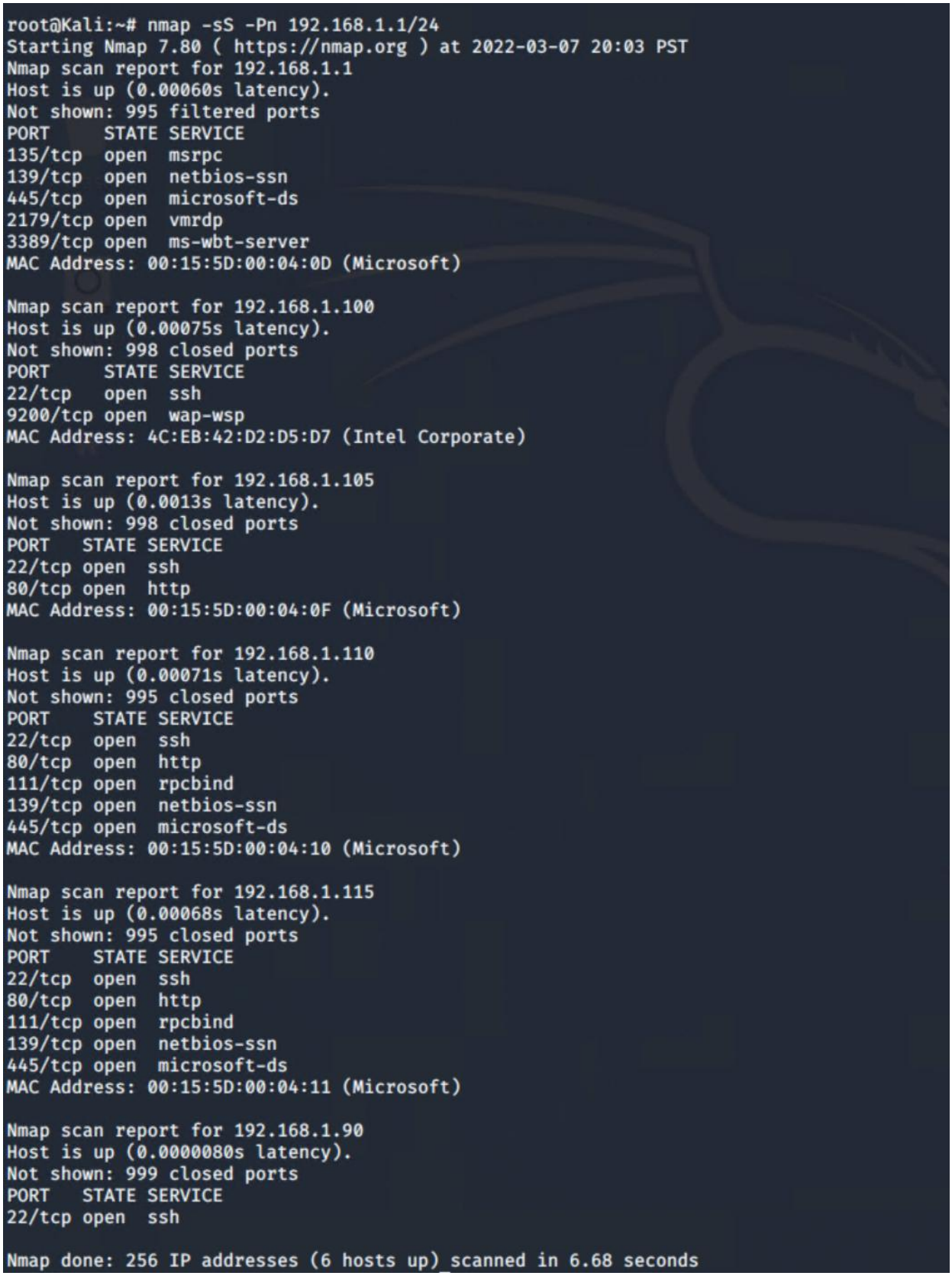
Red Team: Summary of Operations

Table of Contents

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

nmap -sS -Pn 192.168.1.1/24



```
root@Kali:~# nmap -sS -Pn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 20:03 PST
Nmap scan report for 192.168.1.1
Host is up (0.00060s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00075s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00071s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap scan report for 192.168.1.115
Host is up (0.00068s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.68 seconds
```

This scan identifies the services below as potential points of entry:

Target 1

SERVICE	PORT
ssh	22
http	80
rpcbind	111
netbios-ssn	139
microsoft-ds	445

The following vulnerabilities were identified on each target:

Target 1

Port 22

CVE	SEVERITY
CVE-2015-5600	8.5 / High
CVE-2015-6564	6.9 / Medium
CVE-2018-15919	5.0 / Medium
CVE-2017-15906	5.0 / Medium
SSV:90447 (CVE-2016-0777)	4.6 / Medium
CVE-2016-0778	4.6 / Medium
CVE-2021-41617	4.4 / Medium
CVE-2020-14145 (OpenSSH Vulnerability)	4.3 / Medium
CVE-2020-14145 (Huawei EulerOS/SP9)	4.3 / Medium
CVE-2020-14145 (Huawei EulerOS/SP8)	4.3 / Medium

CVE-2020-14145 (Huawei EulerOS/SP5)	4.3 / Medium
CVE-2020-14145 (F5 Networks/F5 Big IP)	4.3 / Medium
CVE-2020-14145	4.3 / Medium
CVE-2015-5352	4.3 / Medium
CVE-2016-0777 (Ubuntu/USN-2869-1)	4.0 / Medium
CVE-2016-0777 (IBM AIX)	4.0 / Medium
CVE-2016-0777 (Debian)	4.0 / Medium
CVE-2016-0777 (AIX 7.2)	4.0 / Medium
CVE-2016-0777 (AIX 7.1)	4.0 / Medium
CVE-2016-0777 (AIX 5.3)	4.0 / Medium
CVE-2016-0777	4.0 / Medium
CVE-2015-6563 (Alpine Linux)	1.9 / Low
CVE-2015-6563	1.9 / Low

PORT 80

CVE	SEVERITY
CVE-2021-44790	7.5 / High
CVE-2021-39275	7.5 / High
CVE-2021-26691	7.5 / High
CVE-2017-7679	7.5 / High
CVE-2017-7668	7.5 / High
CVE-2017-3169	7.5 / High

CVE-2017-3167	7.5 / High
CVE-2018-1312	6.8 / Medium
CVE-2017-15715	6.8 / Medium
CVE-2017-15715 (SUSE)	6.8 / Medium
CVE-2017-15715 (Red Hat)	6.8 / Medium
CVE-2017-15715 (Oracle Linux)	6.8 / Medium
CVE-2017-15715 (Oracle Solaris 11)	6.8 / Medium
CVE-2017-15715 (IBM HTTP Server)	6.8 / Medium
CVE-2018-1312 (Huawei EulerOS/SP3)	6.8 / Medium
CVE-2017-15715 (Huawei EulerOS/SP3)	6.8 / Medium
CVE-2017-15715 (Huawei EulerOS/SP2)	6.8 / Medium
CVE-2018-1312 (Huawei EulerOS/SP2)	6.8 / Medium
CVE-2017-15715 (Huawei EulerOS/SP1)	6.8 / Medium
CVE-2017-15715 (Huawei EulerOS/SP1)	6.8 / Medium
CVE-2017-15715 (FreeBSD)	6.8 / Medium
CVE-2017-15715 (Debian)	6.8 / Medium
CVE-2017-15715 (Centos Linux)	6.8 / Medium
CVE-2017-15715 (Apache HTTPD)	6.8 / Medium
CVE-2017-15715 (Amazon Linux AMI)	6.8 / Medium

CVE-2018-1312 (Alpine Linux)	6.8 / Medium
CVE-2017-15715 (Alpine Linux)	6.8 / Medium
CVE-2021-40438	6.8 / Medium
CVE-2020-35452	6.8 / Medium
CVE-2018-1312	6.8 / Medium
CVE-2017-15715	6.8 / Medium
Server-Side Request Forgery Exploit (CVE-2021-40438)	6.8 / Medium
CVE-2021-44224	6.4 / Medium
CVE-2017-9788	6.4 / Medium
CVE-2019-0217 (Red Hat)	6.0 / Medium
CVE-2019-0217 (IBM HTTP Server)	6.0 / Medium
CVE-2019-0217	6.0 / Medium
CVE-2020-1927	5.8 / Medium
CVE-2019-10098	5.8 / Medium
1337DAY-ID-33577	5.8 / Medium
CVE-2016-5387	5.1 / Medium
SSV:96537 (CVE-2017-9798)	5.0 / Medium
CVE-2018-1303	5.0 / Medium
CVE-2017-15710	5.0 / Medium
CVE-2020-1934	5.0 / Medium
CVE-2017-15710 (Oracle Solaris)	5.0 / Medium
CVE-2017-15710 (IBM HTTP Server)	5.0 / Medium
CVE-2016-8743	5.0 / Medium

CVE-2016-2161	5.0 / Medium
CVE-2016-0736	5.0 / Medium
CVE-2017-15710 (Huawei EulerOS/SP3)	5.0 / Medium
CVE-2017-15710 (Huawei EulerOS/SP2)	5.0 / Medium
CVE-2017-15710 (Centos Linux)	5.0 / Medium
Apache Optionsbleed Scanner	5.0 / Medium
Apache mod_session_crypto	5.0 / Medium
Apache 2.2.34 2.4.27	5.0 / Medium
EDB-ID:42745	5.0 / Medium
EDB-ID:40961	5.0 / Medium
CVE-2021-34798	5.0 / Medium
CVE-2021-26690	5.0 / Medium
CVE-2020-1934	5.0 / Medium
CVE-2019-17567	5.0 / Medium
CVE-2019-0220	5.0 / Medium
CVE-2018-17199	5.0 / Medium
CVE-2018-1303	5.0 / Medium
CVE-2017-9798	5.0 / Medium
CVE-2017-15710	5.0 / Medium
CVE-2016-8743	5.0 / Medium
CVE-2016-2161	5.0 / Medium
CVE-2016-0736	5.0 / Medium
CVE-2015-3183	5.0 / Medium
CVE-2015-0228	5.0 / Medium
CVE-2014-3583	5.0 / Medium
1337DAY-ID-28573	5.0 / Medium

1337DAY-ID-26574	5.0 / Medium
CVE-2018-1302	4.3 / Medium
CVE-2018-1301	4.3 / Medium
CVE-2016-4975	4.3 / Medium
CVE-2019-10092	4.3 / Medium
CVE-2020-11985	4.3 / Medium
CVE-2019-10092	4.3 / Medium
CVE-2020-11985	4.3 / Medium
CVE-2019-10092	4.3 / Medium
CVE-2018-1302	4.3 / Medium
CVE-2018-1301	4.3 / Medium
CVE-2016-4975	4.3 / Medium
CVE-2015-3185	4.3 / Medium
CVE-2014-8109	4.3 / Medium
Exploit for Cross-site Scripting	4.3 / Medium
1337DAY-ID-33575	4.3 / Medium
CVE-2018-1283 (Ubuntu)	3.5 / Low
CVE-2018-1283 (Redhat Linux)	3.5 / Low
CVE-2018-1283 (Oracle Solaris)	3.5 / Low
CVE-2018-1283 (IBM HTTP Server)	3.5 / Low
CVE-2018-1283 (Huawei EulerOS/SP2)	3.5 / Low
CVE-2018-1283 (Centos Linux)	3.5 / Low
CVE-2018-1283	3.5 / Low
CVE-2016-8612	3.3 / Low

Apache mod_session_crypt 2.5	0.0 / None

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 20:13 PST
Nmap scan report for 192.168.1.110
Host is up (0.00073s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/ 6.9     https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/     4.3     https://vulners.com/metasploit/MSF:ILITIES/OPENB
EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITI
VE-2020-14145/  *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITI
VE-2020-14145/  *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITI
VE-2020-14145/  *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/   4.3     https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       MSF:ILITIES/UBUNTU-CVE-2016-0777/       4.0     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/IBM-AIX-CVE-2016-0777/      4.0     https://vulners.com/metasploit/MSF:ILITIES/IBM-AIX-CVE-2
|       MSF:ILITIES/DEBIAN-CVE-2016-0777/       4.0     https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-20
|       MSF:ILITIES/AIX-7.2-OPENSSH_ADVISORY7_CVE-2016-0777/    4.0     https://vulners.com/metasploit/MSF:ILITI
7_CVE-2016-0777/        *EXPLOIT*
|       MSF:ILITIES/AIX-7.1-OPENSSH_ADVISORY7_CVE-2016-0777/    4.0     https://vulners.com/metasploit/MSF:ILITI
7_CVE-2016-0777/        *EXPLOIT*
|       MSF:ILITIES/AIX-5.3-OPENSSH_ADVISORY7_CVE-2016-0777/    4.0     https://vulners.com/metasploit/MSF:ILITI
7_CVE-2016-0777/        *EXPLOIT*
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|       MSF:ILITIES/ALPINE-LINUX-CVE-2015-6563/ 1.9     https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
| vulners:
|   cpe:/a:apache:http_server:2.4.10:
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-3169   7.5     https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       MSF:ILITIES/UBUNTU-CVE-2018-1312/       6.8     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/UBUNTU-CVE-2017-15715/      6.8     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/SUSE-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2017
|       MSF:ILITIES/REDHAT_LINUX-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/REDHA
PLOIT*
|       MSF:ILITIES/ORACLE_LINUX-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/ORACL
PLOIT*
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15715/      6.8     https://vulners.com/metasploit/MSF:ILITIES/ORACL
EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15715/     6.8     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2018-1312/       6.8     https://vulners.com/metasploit/MSF:ILITI
VE-2018-1312/   *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15715/      6.8     https://vulners.com/metasploit/MSF:ILITI
VE-2017-15715/  *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1312/       6.8     https://vulners.com/metasploit/MSF:ILITI
VE-2018-1312/   *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15715/      6.8     https://vulners.com/metasploit/MSF:ILITI
VE-2017-15715/  *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2018-1312/       6.8     https://vulners.com/metasploit/MSF:ILITI
VE-2018-1312/   *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2017-15715/      6.8     https://vulners.com/metasploit/MSF:ILITI
VE-2017-15715/  *EXPLOIT*
|       MSF:ILITIES/FREEBSD-CVE-2017-15715/     6.8     https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-CVE-2
|       MSF:ILITIES/DEBIAN-CVE-2017-15715/      6.8     https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-20
|       MSF:ILITIES/CENTOS_LINUX-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/CENTO
PLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/APACH
PLOIT*
|       MSF:ILITIES/AMAZON_LINUX-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/AMAZO
PLOIT*
|       MSF:ILITIES/ALPINE-LINUX-CVE-2018-1312/ 6.8     https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-
|       MSF:ILITIES/ALPINE-LINUX-CVE-2017-15715/        6.8     https://vulners.com/metasploit/MSF:ILITIES/ALPIN
PLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8     https://vulners.com/cve/CVE-2020-35452
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
```

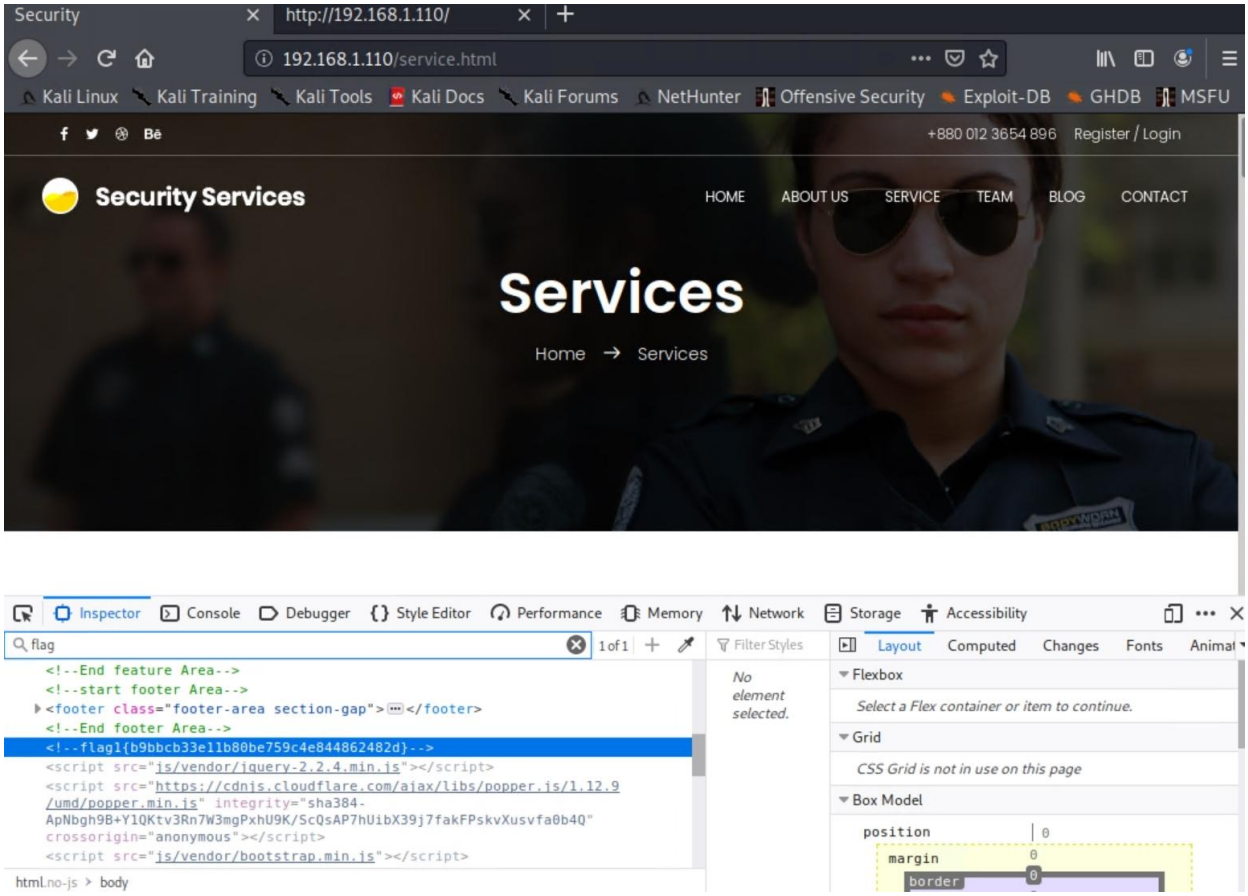
```
|       CVE-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/ 6.0     https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/      6.0     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8     https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       CVE-2016-5387   5.1     https://vulners.com/cve/CVE-2016-5387
|       SSV:96537       5.0     https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       MSF:ILITIES/UBUNTU-CVE-2018-1303/       5.0     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/UBUNTU-CVE-2017-15710/      5.0     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2020-1934/       5.0     https://vulners.com/metasploit/MSF:ILITIES/ORACL
EXPLOIT*
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15710/      5.0     https://vulners.com/metasploit/MSF:ILITIES/ORACL
EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15710/     5.0     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-8743/      5.0     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-2161/      5.0     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-0736/      5.0     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15710/      5.0     https://vulners.com/metasploit/MSF:ILITI
VE-2017-15710/  *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15710/      5.0     https://vulners.com/metasploit/MSF:ILITI
VE-2017-15710/  *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2017-15710/        5.0     https://vulners.com/metasploit/MSF:ILITIES/CENTO
PLOIT*
|       MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED  5.0     https://vulners.com/metasploit/MSF:AUXILIARY/SCA
ED      *EXPLOIT*
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7    5.0     https://vulners.com/exploitpack/EXPLOITPACK:DAED
7       *EXPLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0     https://vulners.com/exploitpack/EXPLOITPACK:C8C2
D       *EXPLOIT*
|       EDB-ID:42745    5.0     https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
|       EDB-ID:40961    5.0     https://vulners.com/exploitdb/EDB-ID:40961      *EXPLOIT*
|       CVE-2021-34798  5.0     https://vulners.com/cve/CVE-2021-34798
|       CVE-2021-26690  5.0     https://vulners.com/cve/CVE-2021-26690
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-17567  5.0     https://vulners.com/cve/CVE-2019-17567
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-1303   5.0     https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-9798   5.0     https://vulners.com/cve/CVE-2017-9798
|       CVE-2017-15710  5.0     https://vulners.com/cve/CVE-2017-15710
|       CVE-2016-8743   5.0     https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-2161   5.0     https://vulners.com/cve/CVE-2016-2161
|       CVE-2016-0736   5.0     https://vulners.com/cve/CVE-2016-0736
|       CVE-2015-3183   5.0     https://vulners.com/cve/CVE-2015-3183
|       CVE-2015-0228   5.0     https://vulners.com/cve/CVE-2015-0228
|       CVE-2014-3583   5.0     https://vulners.com/cve/CVE-2014-3583
|       1337DAY-ID-28573        5.0     https://vulners.com/zdt/1337DAY-ID-28573        *EXPLOIT*
|       1337DAY-ID-26574        5.0     https://vulners.com/zdt/1337DAY-ID-26574        *EXPLOIT*
|       MSF:ILITIES/UBUNTU-CVE-2018-1302/       4.3     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/UBUNTU-CVE-2018-1301/       4.3     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2016-4975/       4.3     https://vulners.com/metasploit/MSF:ILITI
VE-2016-4975/   *EXPLOIT*
|       MSF:ILITIES/DEBIAN-CVE-2019-10092/      4.3     https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-20
|       MSF:ILITIES/APACHE-HTTPD-CVE-2020-11985/        4.3     https://vulners.com/metasploit/MSF:ILITIES/APACH
PLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/        4.3     https://vulners.com/metasploit/MSF:ILITIES/APACH
PLOIT*
|       CVE-2020-11985  4.3     https://vulners.com/cve/CVE-2020-11985
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302   4.3     https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301   4.3     https://vulners.com/cve/CVE-2018-1301
|       CVE-2016-4975   4.3     https://vulners.com/cve/CVE-2016-4975
|       CVE-2015-3185   4.3     https://vulners.com/cve/CVE-2015-3185
|       CVE-2014-8109   4.3     https://vulners.com/cve/CVE-2014-8109
|       4013EC74-B3C1-5D95-938A-54197A58586D     4.3     https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938
|       1337DAY-ID-33575        4.3     https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
|       MSF:ILITIES/UBUNTU-CVE-2018-1283/       3.5     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-20
|       MSF:ILITIES/REDHAT_LINUX-CVE-2018-1283/ 3.5     https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2018-1283/       3.5     https://vulners.com/metasploit/MSF:ILITIES/ORACL
EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2018-1283/      3.5     https://vulners.com/metasploit/MSF:ILITIES/IBM-H
EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1283/       3.5     https://vulners.com/metasploit/MSF:ILITI
VE-2018-1283/   *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2018-1283/ 3.5     https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-
|       CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612   3.3     https://vulners.com/cve/CVE-2016-8612
|_      PACKETSTORM:140265      0.0     https://vulners.com/packetstorm/PACKETSTORM:140265      *EXPLOIT*
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35431/tcp   status
|   100024  1          43780/tcp6  status
|   100024  1          53043/udp   status
|_  100024  1          59400/udp6  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.95 seconds
```

Exploitation

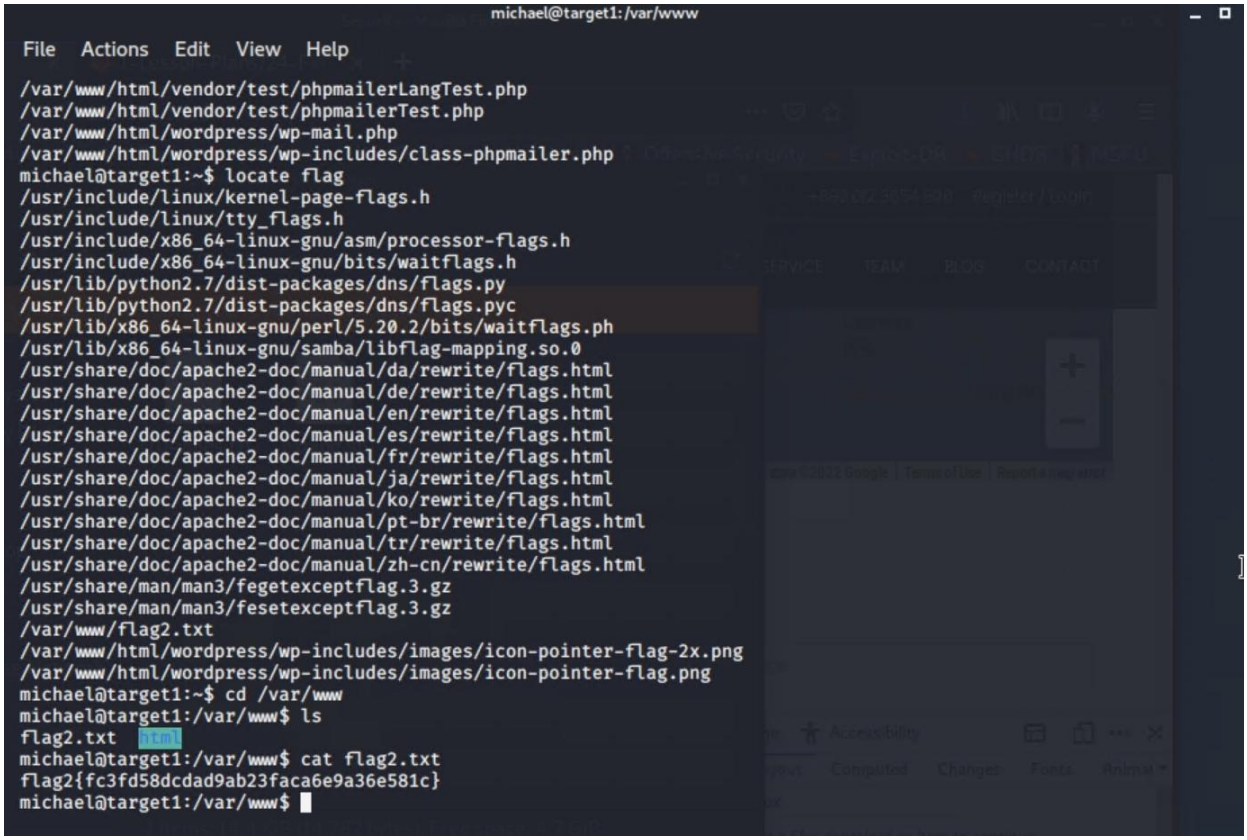
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
    - **flag1.txt: *b9bbcb33e11b80be759c4e844862482d***
        - **Exploit Used**
            - Enumerated the vulnerable WordPress website using the built in developer tools of ‘Inspect Element’ or viewing the ‘Page Source’
            - Right-Clicked to ‘Inspect’ or ‘View Page source’ specifically off the service.html and searched for the flag using ‘flag’.

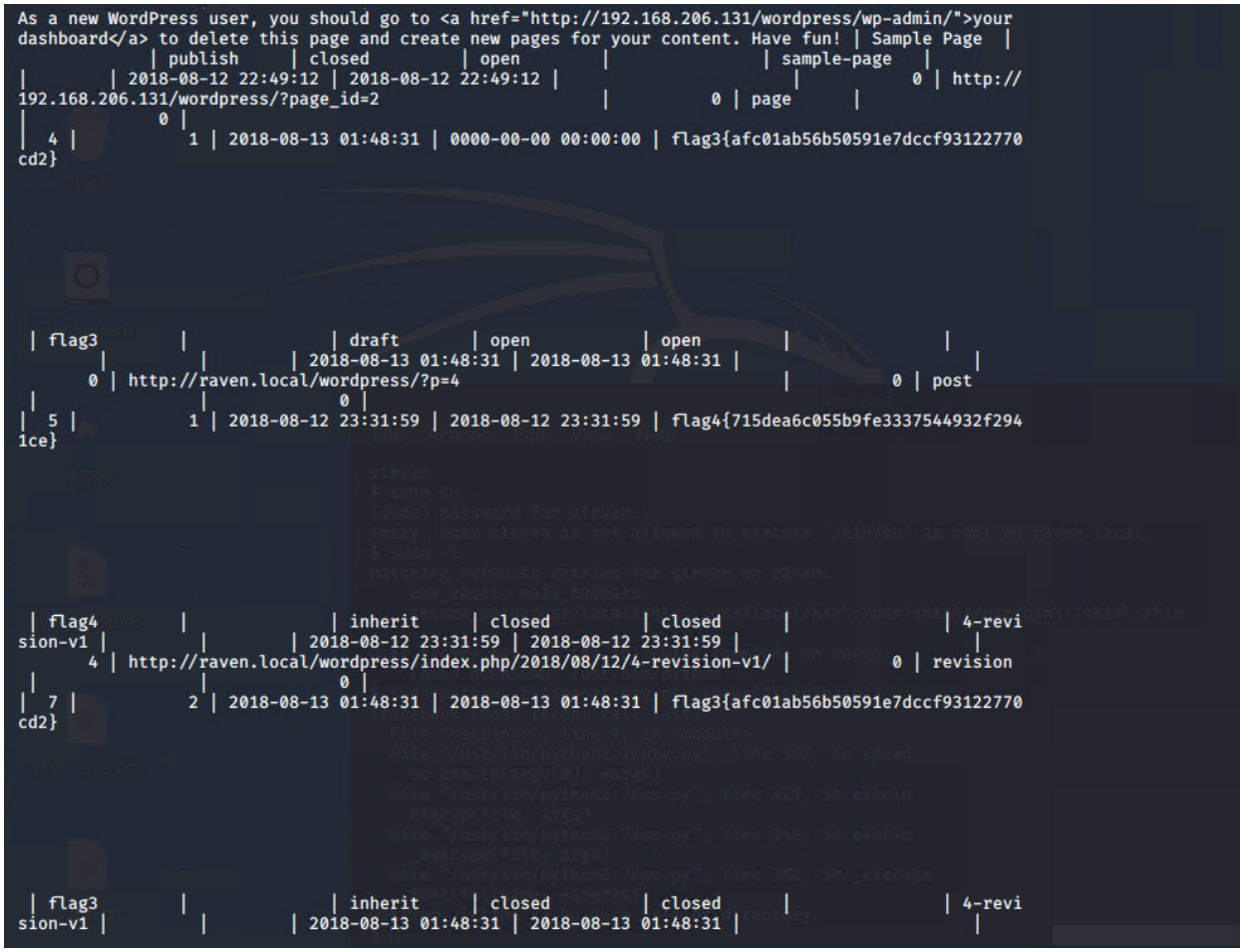


    - **flag2.txt: *fc3fd58dcdad9ab23faca6e9a36e581c***
        - **Exploit Used**
            - Weak SSH passwords and Weak credentials were exploited in order to access the user Michael.
            - ***ssh michael@192.168.1.110 -p 22*** - to connect to the host
            - ***locate flag*** - locating in the hosts files the keyword ‘flag’

- ***cd /var/www*** - redirecting current directory to the path */var/www*
- ***cat flag2.txt*** - after listing with *ls* the location of the file, we use cat to read it out and are retracting the information needed



- **flag3.txt: *afc01ab56b50591e7dccf93122770***
- **flag4.txt: *715dea6c055b9fe3337544933f294***
  - **Exploit Used**
    - Plain text Database Password Access was exploited to access the database information through MySQL from the user that was infiltrated.
    - Upon deeper inspection through the fields in their designated table from the database ‘wordpress’ we are able to find flag 3 and flag 4 in the ‘wp_posts’ table.



```
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your
dashboard</a> to delete this page and create new pages for your content. Have fun! | Sample Page   |
           | publish     | closed          | open          |               | sample-page    |
|         | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                                |          0 | http://
192.168.206.131/wordpress/?page_id=2                       |          0 | page      |
             0 |
|   4 |          1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770
cd2}



 | flag3        |              | draft       | open           | open        |                |
       |         |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                                |
      0 | http://raven.local/wordpress/?p=4                                  |          0 | post
 |                |             0 |
|   5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f294
1ce}



 | flag4        |              | inherit     | closed         | closed      |                | 4-revi
sion-v1 |         |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                                |
      4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ |          0 | revision
 |                |             0 |
|   7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770
cd2}



 | flag3        |              | inherit     | closed         | closed      |                | 4-revi
sion-v1 |         |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                                |
```